9

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/688,397	10/16/2003	Graeme John Proudler	B-5268 621375-8	1309

7590 02/07/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
MORAN, RANDAL D	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/688,397	PROUDLER, GRAEME JOHN	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/16/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-48 are pending in this application.

2. NPL Document TCPA PC Specific Implementation Specification, Version 1.00, pp. 1-70, (September 9, 2001) is unreadable and has not been considered. The remainder of the IDS filed on 10/16/2003 has been considered by the examiner.

Claim Objections

3. **Claims 1, 5, 7, 11, 12, 17, 21, 23 27, 28, 33, 37, and 38** are objected to because of the following informalities:

- Considering **Claims 1**- line 1, **5**- lines 1-2, **7**- lines 1-2, **17**- lines 1, **21**- line 2, **and 23**- line 2, "an hierarchy" should be "a hierarchy."
- Considering **Claims 11, 12, 27, 28, 33, 37, and 38,** "authorisation" contains a spelling error.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 3-5, 17, 19, 21, 29, 33-42, and 45-48** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas et al. (US 4,941,176)** and **Challener (US 2002/0059286)**.

6. Considering **Claims 1 and 17,** Matyas discloses a method of managing an hierarchy of nodes manipulated by processing apparatus (column 2, lines 19-27), the method comprising a step of permitting access to a particular node of the hierarchy (column 2, lines 52-58, column 21, lines 49-53- a control vector is associated with each particular node and defines the usage attributes of that node thereby permitting access to the node)

Matyas does not explicitly disclose allowing access to a particular node only after receiving a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes.

Challener does disclose allowing access to a particular node only after receiving a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes ([0021] lines 14-21, user authorization data of the platform key is a reliable indication that the mechanism has performed access restrictions on the node).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by the mechanism to enforce access restrictions on the node as taught by Challener for the benefit of using keys that have a faster loading time than that of a regular RSA key (Challener-[0020]). The combination would also enable the flexible control of many cryptographic key management functions in the generation, distribution, and use of cryptographic keys, while maintaining a high security standard (Matyas-abstract, lines 33-36).

7. Considering **Claim 33 and 34,** Matyas discloses a processing apparatus comprising a key-handling unit for handling a tree-structured hierarchy (column 2, lines 19-27) in which each non-leaf node comprises a key used to encrypt the or each of its child nodes (column 8, lines 34-69, column 9, lines 1-30, Matyas discloses using a key from the previous node to combine with a random number to encrypt its child node), the hierarchy including, below its top level, a node comprising a particular key associated with a protected process executable by the processing apparatus (column 9, lines 30-44, a master key is kept in the top level of the hierarchy and the regular keys as described above are used to encrypt the child nodes), only after verifying the presence of a benign operating environment within the apparatus for said protected process (column 7, lines 6-16, Figure 1- item 6).

Matyas does not explicitly disclose the key-handling unit being arranged to make said particular key available for use in relation to the protected process upon receipt both of authorization to do so and an indication that the authorization is provided by a trusted source that is arranged to provide this authorization, and to initiate or permit execution of said protected process.

Challener does explicitly disclose the key-handling unit being arranged to make said particular key available for use in relation to the protected process ([0021] lines 14-21) upon receipt both of authorization to do so and an indication that the authorization is provided by a trusted source that is arranged to provide this authorization (Challener- [0024] lines 8-12, [0025] lines 5-8), and to initiate or permit execution of said protected process ([0021] lines 6-21).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas making the key available for use with the protected process upon receipt of authorization that the authorization is from a trusted source and to permit execution of the protected process as taught by Challener for the benefit of using keys that have a faster loading time than that of a regular RSA key (Challener- [0020]). The combination would also enable the flexible control of many cryptographic key management functions in the generation, distribution, and use of cryptographic keys, while maintaining a high security standard (Matyas- abstract, lines 33-36).

8. Considering **Claim 35,** Matyas discloses an apparatus comprising a key-handling unit for handling a tree-structured key hierarchy (column 2, lines 19-27), the key-handling unit being arranged to treat a selected node of the hierarchy as the current root node such that those parts of the hierarchy that can only be reached by ascent from the current root node are inaccessible (column 8, lines 34-69, column 9, lines 1-30, using the parent key and a random number to encrypt the child node makes the parent node the root of the particular tree hierarchy). Matyas does not explicitly disclose the key-handling unit including an arrangement for changing the node of the hierarchy serving as said current root node.

Challener does disclose the key-handling unit including an arrangement for changing the node of the hierarchy serving as said current root node ([0021] lines 23-27).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Matyas by having an arrangement to change the current root node of the hierarchy as taught by Challener for the benefit of not having to migrate all keys below it explicitly. This process is done automatically in a relatively small amount of time compared to having to migrate all keys (Challener- [0021] lines 30-35).

9. Considering **Claims 3 and 19,** the combination of Matyas and Challener discloses mechanism is a protected process executing in a benign operating

environment within the apparatus (Matyas- column 7, lines 6-16, Figure 1- item 6), the method further comprising using a trusted source to establish or initiate establishment of said mechanism and to generate said reliable indication accordingly (Matyas- column 2, lines 19-27, Challener- [0024] lines 8-12, [0025] lines 5-8).

10. Considering **Claims 4 and 29,** the combination of Matyas and Challener discloses each non-leaf node of said hierarchy comprises a key used to encrypt the or each of its child nodes (Matyas- column 8, lines 34-69, column 9, lines 1-30, Matyas discloses using a key from the previous node to combine with a random number to encrypt its child node), said particular node being a node below the top level of the hierarchy that comprises a particular key associated with said protected process (Matyas- column 9, lines 30-44, a master key is kept in the top level of the hierarchy and the regular keys as described above are used to encrypt the child nodes), this key being made available for use in relation to the protected process upon said reliable indication being received (Matyas- Figure 1- item 6, Challener- [0025] lines 5-8).

11. Considering **Claims 5 and 21,** the combination of Matyas and Challener discloses particular key forms the root of a hierarchy of cryptographically-protected objects associated with the protected process (Matyas- column 8, lines 34-69, column 9, lines 1-30, using the parent key and a random number to

encrypt the child node makes the parent node the root of the particular tree hierarchy).

12. Considering **Claim 36,** the combination of Matyas and Challener discloses the arrangement for changing the current root node is enabled to do so only upon a predetermined set of at least one condition being met (Challener- [0007]).

13. Considering **Claim 37,** the combination of Matyas and Challener discloses at least one predetermined condition comprises the receipt of an authorization value indicative of digital data ([0021] lines 23-27, all keys and requests with the cryptographic processor would be digital data).

14. Considering **Claim 38,** the combination of Matyas and Challener discloses authorization value is a digest of a protected process associated with the node that is intended to be the new current root node (Challener- p.5 right column, lines 14-17).

15. Considering **Claim 39,** the combination of Matyas and Challener discloses at least one predetermined condition comprises that a protected process associated with the node that is intended to be the new current root node is about to be run by the apparatus (Challener- [0021], if you are attempting to migrate keys and access them, you are also intending to unlock the nodes and run the process).

16. Considering **Claim 40,** the combination of Matyas and Challener discloses at least one predetermined condition comprises that any other currently-activated processes running on the apparatus are benign (Matyas- Figure 1- item 6, any process running within the secure boundary would also be considered secure).

17. Considering **Claim 41,** the combination of Matyas and Challener does not explicitly disclose at least one predetermined condition comprises that the key-handling apparatus is requested to change the current root node by a root of trust of the apparatus.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas, Challener, and Kocher by the root change request coming from a root of trust as is well known in the art for the benefit of having a set of unconditionally trusted functions that must work properly no matter what software is executing on the platform, in order to be immune to software attacks. Ideally, it should also be immune to physical attack, to avoid the need to trust an owner or user of a platform.

18. Considering **Claim 42,** the combination of Matyas and Challener discloses the node at the head of the hierarchy as judged without regard to which node is the current root node, forms said current root node upon start of the apparatus

(Challener- Fig. 5- item 501, upon start-up, the storage root key is always considered the current root node).

19. Considering **Claim 45,** the combination of Matyas and Challener discloses the key-handling unit is a Trusted Platform Module according to the TCPA architecture (Challener- [0003]).

20. Considering **Claim 46,** the combination of Matyas and Challener discloses the key-handling unit is arranged to indicate the current root node by signing a value associated with the node using an identity key associated with the key-handling unit (Challener- [0028], [0029], the non-migratable storage key is used to create a signature that would be used to identify it to the chip).

21. Considering **Claim 47,** the combination of Matyas and Challener discloses the key-handling unit is so arranged that only a particular type of key node (Challener [0021] lines 24-27, only the key set to be migrated can be used as the current root node) herein a dynamic key node, can be used as the current root node in addition to the node at the head of the hierarchy as judged without regard to which node is the current root node (Fig 5, the storage root key can be used as the root as well as the migratable key (i.e. the dynamic root)).

22. Considering **Claim 48,** the combination of Matyas and Challener discloses the key-handling apparatus is arranged, upon receipt of a corresponding command, to generate a dynamic root node as a node of said key hierarchy (Challener-[0007]).

23. **Claims 2, 6, 7, 9-14, 16, 18, 22, 23, 25-30, and 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas, Challener** in further view of **Kocher et al. (US 6,289,455)**, hereafter "Kocher."

24. Considering **Claims 2, 6, 18, and 22,** Matyas and Challener do not disclose step is carried out in a tamper-resistant hardware module.

Kocher does disclose the step is carried out in a tamper-resistant hardware module (column 2, lines 44-50).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas and Challener by the tamper-resistant hardware module as taught by Kocher for the benefit of preventing the misuse of decryption keys. To prevent the misuse of decryption keys, cryptographic hardware used to mange content decryption keys must be tamper-resistant (Kocher- column 1, lines 23-25).

25. Considering **Claims 7 and 23,** the combination of Matyas, Challener, and Kocher discloses particular key forms the root of a hierarchy of cryptographically-

protected objects associated with the protected process (Matyas- column 8, lines 34-69, column 9, lines 1-30, using the parent key and a random number to encrypt the child node makes the parent node the root of the particular tree hierarchy).

26. Considering **Claims 9 and 25,** the combination of Matyas, Challener, and Kocher discloses the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendant nodes are carried out within said module (Matyas- Figure 1, column 7, lines 6-16, Kocher- column 2, lines 44-50), the module responding to the trusted source providing said reliable indication in respect of said protected process (Challener- ([0021] lines 14-21, user authorization data of the platform key is a reliable indication that the mechanism has performed access restrictions on the node) to internally store a release indicator in respect of said particular node (Matyas- Figure 16- item 14), descendants of said particular node being tagged with an identifier of said particular node (Matyas- column 8, lines 34-69, column 9, lines 1-30, each node is encrypted based on information from a parent and given a key, i.e. being tagged) and the module only permitting access to a said descendant of said particular node when the identifier associated with the node concerned corresponds to a stored release indicator (Matyas- column 8, lines 34-69, column 9, lines 1-30, only when you have the parent key and the child key (i.e. the indicator) can you access the node) .

27. Considering **Claims 10 and 26,** the claims are rejected for the same reasons as Claims 5 and 21 respectively.

28. Considering **Claims 11 and 27,** the combination of Matyas, Challener, and Kocher discloses access to said particular node is further conditional upon presentation of an authorization (Matyas- column 8, lines 32-34).

29. Considering **Claims 12 and 28,** the combination of Matyas, Challener, and Kocher discloses authorization is a digest of the protected process, the trusted source calculating this digest from the protected process code to be executed (Challener- p. 5- right column, lines 14-17).

30. Considering **Claims 13 and 29,** the combination of Matyas, Challener, and Kocher do not explicitly disclose trusted source is a hardware root of trust. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas, Challener, and Kocher by the trusted source being a hardware root of trust as is well known in the art for the benefit of having a set of unconditionally trusted functions that must work properly no matter what software is executing on the platform, in order to be immune to software attacks. Ideally, it should also be immune to physical attack, to avoid the need to trust an owner or user of a platform.

31. Considering **Claims 14 and 30,** the combination of Matyas, Challener, and Kocher discloses trusted source is a protected compartment operating system executing on the apparatus (Matyas- Figure 1).

32. Considering **Claims 16 and 32,** the combination of Matyas, Challener, and Kocher discloses the tamper-resistant module (Kocher- column 2, lines 44-50) is a Trusted Platform Module according to the TCPA architecture (Challener- [0003]).

33. **Claims 43 and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas, Challener,** in further view of **Pierce et al. (US 2003/0084292),** hereafter "Pierce."

34. Considering **Claims 43 and 44,** the combination of Matyas and Challener does not discloses the key-handling unit is arranged to hold the current root node internally in unencrypted form at least whilst it remains the current root node. Pierce does disclose the key-handling unit is arranged to hold the current root node internally in unencrypted form at least whilst it remains the current root node ([0031], lines 1-4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas and

Challener by the ability to hold the current root node internally in the TPM in unencrypted form as taught by Pierce for the benefit of increasing the security associated with an electronic message without having to perform a handshaking sequence or maintaining state information ([0022] lines 1-6).

35. **Claims 8, 15, 24, and 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas, Challener, Kocher,** in further view of **Pierce.**

36. Considering **Claims 8 and 24,** the combination of Matyas, Challener, and Kocher does not disclose particular key is made available by revealing it unencrypted outside of said module to the protected process, the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendant nodes, being carried out by said protected process outside of said module.

Pierce does disclose particular key is made available by revealing it unencrypted outside of said module to the protected process ([0019] lines 5-13, [0020] lines 5-12]), the cryptographic use of said particular key and the cryptographic operations for accessing any of its descendant nodes, being carried out by said protected process outside of said module ([0021]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas, Challener, and Kocher by the ability to reveal unencrypted keys outside of said module to

the protected process as taught by Pierce for the benefit of increasing the security associated with an electronic message without having to perform a handshaking sequence or maintaining state information ([0022] lines 1-6).

37. Considering **Claims 15 and 31,** the combination of Matyas, Challener, Kocher, and Pierce discloses the tamper-resistant module holds (Kocher- column 2, lines 44-50), in unencrypted form the top-level node of said hierarchy (Pierce- ([0019] lines 5-13, [0020] lines 5-12]), the other nodes of the hierarchy being stored in encrypted form separately from the key-handling unit when not being used (Matyas- Figure 1- item 18 and 22).

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 7,131,010 - hierarchal key tree structure.
- US 6,061,684 – file management using a hierarchical structure.
- US 2003/0138105 – key storage.
- US 2002/0104001 – using parent nodes to encrypt child nodes.
- US 7,017,189 – multi-level rights management.
- Wallner, D. National Security Agency, Request for Comments 2627. Key management for multicast systems. June 1999.

39 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
RDM
1/30/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100